What is Claimed is:

Sub A3

~~1. A portable terminal for encrypting information, the portable terminal comprising:~~

~~means for generating a new key for each transaction, wherein the new key is generated using one or more properties of the portable terminal.~~

~~2. A portable terminal according to claim 1, wherein the new key is generated when the transaction is executed.~~

~~3. A portable terminal according to claim 1, wherein the one or more properties of the portable terminal include the date and time settings.~~

~~4. A terminal according to claim 1, further comprising means for generating a unique challenge in addition to the new key so that a unique challenge can be issued for each transaction.~~

~~5. A method of encrypting information in a portable terminal, the method comprising the steps of:~~

~~using one or more properties of the portable terminal to obtain a sequence of values; and~~

~~generating a new key based on the sequence of values.~~

~~6. A method according to claim 5, further comprising the step of:~~

~~generating a unique challenge value based on the sequence of values.~~

7. A method according to claim 5, further comprising the steps of:

encrypting the new key and the challenge value using a public key issued by a host; and

transmitting the encrypted new key and challenge value to the host.

8. A method of communicating encrypted information between a portable terminal and a self-service terminal, the method comprising the steps of:

using one or more properties of the portable terminal to obtain a sequence of values;

generating a new key based on the sequence of values;

generating a challenge value based on the sequence of values;

encrypting the new key and the challenge value using a public key; and

transmitting the encrypted key and challenge value to the self-service terminal.

9. A method according to claim 8, further comprising the steps of:

generating a new challenge value at the self-service terminal;

encrypting the generated challenge value using the new key;

transmitting the encrypted challenge value to the portable terminal; and

awaiting a correct response to the transmitted challenge value being transmitted by the portable terminal before accepting any subsequent transaction at the self-service terminal.

~~10. A transaction system comprising:~~

~~a self-service terminal;~~

~~a portable terminal which is operable to use one or more properties of the portable terminal for (i) obtaining a sequence of values, and (ii) generating a new key based on the sequence of values; and~~

~~means for enabling the portable terminal and the self-service terminal to intercommunicate using the new key.~~

~~11. A method of determining if a self-service terminal is an authentic terminal, the method comprising the steps of:~~

~~using one or more properties of a portable terminal to obtain a sequence of values;~~

~~generating a new key based on the sequence of values;~~

~~generating a challenge value based on the sequence of values;~~

~~encrypting the new key and challenge value using a public key provided by an institution;~~

~~transmitting the encrypted key and challenge to the self-service terminal;~~

~~receiving a response from the self-service terminal, decrypting the response using the new key; and~~

~~halting any further transmission unless the decrypted response includes a correct reply to the challenge value.~~

Add A4